

Annual CPNI Certification
47 C.F.R. §64.2010(e)
EB Docket No. 06-36

Received & Inspected

FEB 23 2010

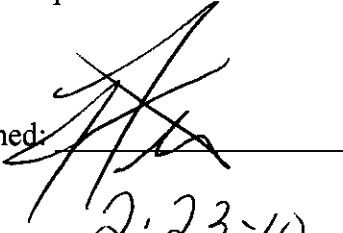
FCC Mail Room

Name of Company: Bitwise Communications, Inc. a/k/a OmniLEC
Form 499 Filer ID: 822650
Name of Signatory: John Furton
Title of Signatory: Vice President

I, John Furton, hereby certify that I am an officer of Bitwise Communications, Inc. a/k/a OmniLEC ("Bitwise") and that I am authorized to make this certification on behalf of Bitwise. I have personal knowledge that Bitwise has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules, to the extent that such rules apply to Bitwise or to any of the information obtained by Bitwise. *See 47 C.F.R. §64.2001 et seq.*

Attached to this certification is an the company's internal policy statement explaining Bitwise's procedures to ensure that it complies with the requirements set forth in §64.2001 *et seq.* of the Commission's rules to the extent that such requirements apply to Bitwise or to the information obtained by Bitwise.

Bitwise has not taken any actions against data brokers before state commissions, state or federal courts, or the FCC in the past year. Bitwise has not received any customer complaints in the past year concerning the unauthorized release of CPNI. Bitwise has no information, other than information that has been publicly reported, regarding the processes that pretexters are using to attempt to access CPNI.

Signed: 

Date: 2.23.10

No. of Copies rec'd 0
List ABCDE

Received & Inspected

FEB 23 2010

FCC Mail Room



CPNI

Policies & Procedures Manual

February 23, 2009

Introduction

Under FCC regulations, all telecommunications carriers are required to protect the privacy of their customers. The "OmniLEC CPNI Policies & Procedures" manual has been put into place in order to ensure OmniLEC follows the FCC privacy guidelines. A copy of the complete CPNI Compliance Manual, issued by the FCC, has been electronically issued to every employee and is posted in every department of the OmniLEC office.

Customer Proprietary Network Information, or CPNI, is certain customer information obtained by a telecommunications provider during the course of providing service to a customer. This includes information relating to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier. CPNI may also include information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

According to the FCC, CPNI encompasses "where, when and to whom" a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent to which the service is used.

CPNI also includes information typically contained in Call Detail Records, such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls. It also includes the additional services and features purchased by the consumer, such as call waiting, Caller ID, etc. CPNI, therefore, contains not only private, personal information, but commercially-sensitive information, as well.

CPNI does not include a customer's name, phone number and address aggregate customer information. Also not included under the definition is "subscriber list information" when included in a telephone directory or publicly available through other means. However, the names, addresses, and telephone numbers of UNLISTED customers are not subscriber list information.

Failure to comply with the guidelines listed in the OmniLEC CPNI Policies & Procedures and the CPNI Compliance Manual will result in the following disciplinary actions:

- 1st offense – written warning will be issued
- 2nd offense – employee termination

Customer Interaction

Customer CPNI Protection Methods

1. CPNI information cannot be visible or accessible when unattended.
2. Customers can not be allowed into an office area where other customer's CPNI information is visible either on a desktop or on a computer.
3. When service is established, an account password is required to activate a customer account.

Customer Authentication Methods

1. CPNI information cannot be provided, via the telephone, without providing the customer's pre-established account password.
2. CPNI information can be provided by mail to the address of record or to the phone number of record.
3. Access to CPNI information can be provided if a valid photo ID is presented by either the account owner or a contact listed on the account.

Customer Notification of CPNI Changes

1. Customers will be automatically emailed a notification when the following items are changed on their account:
 - a. Password modification
 - b. Address of record change or creation
 - c. Online password or auto pay changes
 - d. Online payment is made on account
 - e. Password Retrieval for Customers through the OmniLEC website

Sales

Sales and Marketing Campaign Approval

1. All sales and marketing campaigns are to be submitted on form S-101(appendix A) to the OmniLEC CEO for approval. If customers' CPNI information is to be used in the campaign, a completed and signed form O-101 (appendix B), per customer, must accompany the S-101 form upon submission. Sales and marketing campaigns WILL NOT be approved without the appropriate paperwork completed and signed. Electronic and verbal submissions WILL NOT be accepted.
2. Forms S-101's and O-101's will be submitted to and maintained by the accounting department for no less than one (1) year.

Permissible Use of CPNI in Sales

1. Sales staff may use or disclose CPNI in order to market services that are within the same category of services to which the customer presently subscribes. For example, sales staff can use or disclose CPNI information to sell additional local services to an existing local service subscriber. Sales staff may disclose CPNI without prior authorization in order to offer additional services associated with subscribed services, such as customer premise equipment, call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion. Likewise sales staff can use CPNI to market services formerly known as adjunct-to-basic services, including, but not limited to, speed-dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features. Further, if a customer is subscribed to more than one category of service offered by a carrier (i.e., both local and wireless services), a carrier is permitted to share CPNI between the different affiliated entities that provide the subscribed services, provided the customer subscribes to each service.
2. Please refer to the CPNI compliance Manual's "Use of CPNI without Customer Approval" page 4 and "Frequently Asked Questions" page 9.

Non-Permissible Use of CPNI in Sales

1. Sales staff are not permitted to disclose CPNI without prior authorization to a service provider to whom a customer is not already subscribed. Sales staff are also prohibited from using CPNI to identify or track customers that call competing service providers. For example, staff may not use CDR records to track all customers that call local service competitors.

2. Please refer to the CPNI compliance Manual's "Use of CPNI without Customer Approval" page 4.

OmniLEC Company CPNI Policies

Opt-in

1. Before OmniLEC will share or disclose CPNI for the purpose of marketing both communications-related and non-communications-related services with joint venture partners, independent contractors, or third parties separate from OmniLEC, an "opt-in" (form O-101) approval will be obtained from each customer involved. This means that before OmniLEC will disclose information to a third party, OmniLEC will seek informed consent in a formally executed notification returned by the customer.
2. Completed form O-101's will be submitted to and maintained by the accounting department for no less than one (1) year.

Opt-out Mechanism Failure

1. OmniLEC will provide written notice using Form O-103 (Appendix D) within five (5) business days to the FCC of any instance where opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Unauthorized Access to CPNI

1. Should unauthorized access to a customer's CPNI be obtained, OmniLEC will send an electronic notification to the United States Secret Service ("USSS") and the Federal Bureau of Investigations ("FBI") through the FCC link <http://www.fcc.gov/eb/cpni>. This notification will be sent within seven (7) business days after reasonable determination that a breach has occurred and will contain the following information:
 - a. Dates of discovery and notification
 - b. Detailed description of the CPNI that was the subject of the breach
 - c. Circumstances of the breach
2. OmniLEC will then notify the customer of the unauthorized access.
3. A copy of the notification (Appendix C) will be submitted to and maintained by the accounting department for no less than two (2) years.

Additional Measures to Protect CPNI Information

1. The servers that run OmniLEC databases are locked down from access outside of the OmniLEC network. This means that unless you are directly connected to the OmniLEC network, you would be unable to gain remote administration to these servers.
2. OmniLEC utilizes VPN for all devices that require remote administration. A VPN client certificate, that is specific to the VPN firewall on the OmniLEC network, is required for OmniLEC network technicians to gain access to anything on the OmniLEC network through the Internet. Access to the OmniLEC network, without a VPN client certificate, is not a possibility.
3. OmniLEC has implemented real-time monitoring of our entire network core for intrusion detection and remote attacks. OmniLEC has setup predefined automatic email responses to a vast number of known threats. This allows OmniLEC network technicians to monitor the network 24 hours a day, 7 days a week. Ninety-nine percent of OmniLEC network attacks are stopped by automatic scripted responses.

-- Appendix A --



Form S-101

Sales and Marketing Campaign Proposal

Name of Company Presenting the Campaign:

Start and End Date: _____

Will this campaign require the use of CPNI information? ☐ Yes ☐ No

**** Signed Form O-101's must be attached if CPNI information is to be used ****

If yes, what type of CPNI will be used in the campaign?

What products and services will be offered in this campaign?

Submitted By: _____

Approved By: _____

(CEO Signature)

Date: _____

Date: _____

-- Appendix B --



Form O-101

Customer Proprietary Network Information

Dear Valued Customer,

In order to continue to provide excellent products and services, OmniLEC gathers information about the quality, type, destination, technical configurations, and amount of products and services you use. This information is called Customer Proprietary Network Information ("CPNI").

Please be advised that under federal regulations, you have a right, and OmniLEC has a duty, to protect the confidentiality of your CPNI. OmniLEC will not disclose or sell your CPNI without receiving prior authorization, or unless required to do so by operation of law. We will also discontinue using your information upon request.

To continue to serve you in the most effective and efficient manner, we would like to use your CPNI for purposes of determining the best products and services that will benefit you. By opting-in, OmniLEC may also disclose, share or permit access to your CPNI on a limited, as-needed basis with trusted agents and contractors that assist us in providing you with communications-related services.

Please note that we will continue to rely upon this authorization until you have notified us of any limitations on the use of your CPNI. Also, please be aware that denial of authorization will not affect your current telecommunications service.

In order for us to begin better serving you, please check the appropriate box below and return this form to our mailing address:

OmniLEC
331 Fulton St. Suite 300
Peoria, IL 61602

- ☐ I authorize OmniLEC to share my CPNI information with trusted agents.
- ☐ I do not authorize OmniLEC to share my CPNI information with trusted agents.

(Signature of Authorized Person)

Date: _____

-- Appendix C --



Form O-102

Unauthorized Access Notification

OmniLEC
331 Fulton St. Suite 300
Peoria, IL 61602

Date of Access: _____

Date of Discovery: _____

Date of Law Enforcement Notification: _____

Date of Customer Notification: _____

Submitted By: _____

Please give a detailed description of the CPNI that was the subject of the breach:

Please describe the circumstances of the breach:

-- Appendix D --



OmniLEC
331 Fulton St. Suite 300
Peoria, IL 61602

Date: _____

Submitted By: _____

Please give a detailed description of how the Opt-out Mechanism Failed:

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

FEB 23 2010

Accompanying Statement of Annual CPNI Compliance Certification

FCC Mail Room

Indicate below (X) whether the Company has taken any or all of the following actions to protect against the unlawful disclosure of CPNI.

Employee Training and Discipline

- ☒ Trained all employees and personnel as to when they are and are not authorized to use CPNI.
- ☒ Instituted an express disciplinary process for unauthorized use of CPNI.

Sales and Marketing Campaign Approval

- ☒ Guaranteed that all sales and marketing campaigns are approved by management.

Record-Keeping Requirements

- ☒ Established a system to maintain a record of all sales and marketing campaigns that use their customers' CPNI, including marketing campaigns of affiliates and independent contractors.
- ☒ Ensured that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- ☒ Made certain that these records are maintained for a minimum of one (1) year.

Establishment of a Supervisory Review Process

- ☒ Established a supervisory review process for all outbound marketing situations.
- ☒ Certified that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

Opt-In

- ☒ Guaranteed that the Company only disclosed CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving "opt-in" approval from a
- ☒ Verified that the Company enters into confidential agreements with joint venture partners, independent contractors or any other third party when releasing CPNI.

Opt-Out Mechanism Failure

- ☒ Established a protocol through which the Company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not work properly, to such a

Compliance Certificates

- ☒ Executed a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the
- ☒ Executed a statement detailing how operating procedures ensure compliance with CPNI regulations.

- ☒ Executed a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

Customer Authentication Methods

- ☒ Instituted customer authentication methods to ensure adequate protection of customers' CPNI. These protections only allow CPNI disclosure in accordance with the following methods:
- ☒ Disclosure of CPNI information in response to a customer providing a pre-established password;
 - ☒ Disclose of requested CPNI to the customer's address or phone number of record; and
 - ☒ Access to CPNI if a customer presents a valid photo ID at the carrier's retail location.

Customer Notification of CPNI Changes

- ☒ Established a system under which a customer is notified of any change to CPNI. This system, at minimum, notifies a customer of CPNI access in the following circumstances:
- password modification;
 - a response to a carrier-designed back-up means of authentication;
 - online account changes; or
 - address of record change or creation.

Notification of Law Enforcement and Customers of Unauthorized Access

- ☒ Established a protocol under which the appropriate Law Enforcement Agency ("LEA") is notified of any unauthorized access to a customer's CPNI.
- ☒ Ensured that all records of any discovered CPNI breaches are kept for a minimum of two (2) years.